UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/670,604	09/26/2003	Tetsuro Motoyama	240204US28	1499

22850 7590 06/01/2007

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SIKRI, ANISH	

ART UNIT	PAPER NUMBER
2143	

NOTIFICATION DATE	DELIVERY MODE
06/01/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/670,604	MOTOYAMA, TETSURO	
	Examiner	Art Unit	
	Anish Sikri	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 September 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :12/29/03, 04/27/04, 11/09/04, 3/18/05, 5/24/05, 12/21/05, 12/05/06.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement submitted on 12/29/03, 04/27/04, 11/09/04, 3/18/05, 5/24/05, 12/21/05, 12/05/06 has been considered by the Examiner and made of record in the application file.

Drawings

New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because Fig 10-24 are not labeled properly, some of the drawings use hand written labels and some drawings do not have any labels. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6,8,9,11-18, 20, 21, 23-30, 32, 33, 35-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Ramberg et al (US Pub 20030014505 A1).

Consider **Claim 1**, Ramberg et al clearly discloses a method of storing information configured to be used for a plurality of communication protocols to access a monitored device among distinct devices communicatively coupled to a network (Ramberg et al, [0024]), comprising: retrieving, from a first memory, information for accessing the device using at least one communication protocol supported by the device (Ramberg et al, [0038]) (It clearly shows that the management information base contains the information about the sets of objects, and provides information about each object – including its structure and relationship with other objects);

Storing, in a second memory, the information for accessing the device retrieved from the first memory (Ramberg et al, [0038]-[0039]) (There is also a MIB on the device, which tells SNMP agents information about the devices;

Selecting a communication protocol among the plurality of communication protocols (Ramberg et al, [0024], [0099]); and accessing the device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory (Ramberg et al, [0038]-[0039]). It clearly shows on how monitoring systems employ plurality of communication protocols to be used to monitor devices in the network. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 2**, and as applied to claim 1 above, Ramberg et al clearly discloses the method wherein the retrieving step comprises: accessing a memory external to a monitoring computer to obtain the information for accessing the device (Ramberg et al, [0025], [0038], [0039]). It clearly shows on the use of remote computing system to monitor devices in the network. The management information base is also tied with the application which monitors the devices on the network via SNMP (Ramberg et al, [0039]).

Consider **Claim 3**, and as applied to claim 1 above, Ramberg et al clearly discloses the method, wherein the selecting step comprises: selecting a communication protocol among SNMP, HTTP, and FTP (Ramberg et al, [0024], [0099]). It clearly shows that few of the protocols, which can be used for monitoring devices, comprises of the protocols SNMP, HTTP and FTP. The monitoring systems translate information

within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 4**, and as applied to claim 1 above, Ramberg et al clearly discloses the method, wherein the retrieving step comprises: retrieving, from the first memory, at least one of a username and a password for accessing the device using FTP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use passwords on the devices in the network when accessing them for monitoring.

Consider **Claim 5,** and as applied to claim 1 above, Ramberg et al clearly discloses wherein the retrieving step comprises: retrieving, from the first memory, at least one of a community name and a password for accessing the device using SNMP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use of SNMP along with passwords for monitoring devices in the network.

Consider **Claim 6**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the retrieving step comprises: retrieving, from the first memory, an IP address of the device (Ramberg et al, [0046]). It clearly shows that the devices in the network have an IP address.

Consider **Claim 7**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the second memory comprises a vector of parameter name and

parameter value paris for each of the plurality of communication protocols (Ramberg et al, [0055], [0056]). The SNMP subagents in Ramberg et al's invention uses routines as vectors, as they can used with other programs (Ramberg et al, [0055]). The routines are stored separately as files, and are pointed to when being used (Ramberg et al, [0055]).

Consider **Claim 8**, and as applied to claim 1 above, Ramberg et al clearly discloses the storing step comprises: storing the information for accessing the device in a device software object associated with the device (Ramberg et al, [0040], [0044]-[0045]). It clearly shows that device data is captured from the device and stored in a database.

Consider **Claim 9**, and as applied to claim 8 above, Ramberg et al clearly discloses wherein the device software object is stored in a random-access memory unit of a monitoring computer (Ramberg et al, [0051]). It clearly shows that during monitoring the application software is incorporating the use of system memory. The remote HTML browser which is the remote monitoring console runs on computer, UNIX workstation, host computer etc. These systems have random-access memory unit to function (Ramberg et al, [0051]).

Consider **Claim 10**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the retrieving step comprises: accessing the first memory using

virtual functions associated with an abstract software class (Ramberg et al [0040]-[0041], [0047]). Ramberg et al clearly shows that the platform devices can be managed by the use of Dynamic User Inteface, as it uses XML. And the XML provides a data standard to encode the content, semantics, and schemata for communication. The Java system management can also be used (which contains classes) for communication with SNMP agents [0049].

Consider **Claim 11,** and as applied to claim 1 above, Ramberg et al clearly discloses wherein the accessing step comprises: transmitting to the device, information stored in the second memory necessary to access the device using the selected communication protocol (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows on the usage of memory on the system(s) when monitoring functionality is carried out when accessing the device via SNMP.

Consider **Claim 12**, and as applied to claim 11 above, Ramberg et al clearly discloses wherein the accessing step comprises: receiving, by the device, the transmitted information; and processing, by the device, the received information (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows that during monitoring, both the system monitor and the monitored devices transmit information to each other and vice-versa.

Consider **Claim 13**, Ramberg et al clearly discloses a system of storing information configured to be used for a plurality of communication protocols to access a monitored device among distinct devices communicatively coupled to a network (Ramberg et al, [0024]), comprising: means of retrieving, from a first memory, information for accessing the device using at least one communication protocol supported by the device (Ramberg et al, [0038]) (It clearly shows that the management information base contains the information about the sets of objects, and provides information about each object – including its structure and relationship with other objects);

Means of storing, in a second memory, the information for accessing the device retrieved from the first memory (Ramberg et al, Page 1, [0038]-[0039]) (There is also a MIB on the device, which tells SNMP ages information about the devices);

Means for selecting a communication protocol among the plurality of communication protocols (Ramberg et al, Page 1, [0024], [0099]); and means for accessing the device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory (Ramberg et al, [0038]-[0039]). It clearly shows on how monitoring systems employ plurality of communication protocols to be used to monitor devices in the network. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 14**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for accessing a memory external to a monitoring computer to obtain the information for accessing the device (Ramberg et al, [0025], [0038], [0039]). It clearly shows on the use of remote computing system to monitor devices in the network. The management information base is also tied with the applications which monitors the devices on the netweork va SNMP (Ramberg et al, [0039]).

Consider **Claim 15**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for selecting step comprises: means for selecting a communication protocol among SNMP, HTTP, and FTP (Ramberg et al, [0024], [0099]). It clearly shows that few of the protocols which can be used for monitoring devices comprises of the protocols SNMP, HTTP and FTP. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 16**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for retrieving, from the first memory, at least one of a username and a password for accessing the device using FTP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use passwords on the devices in the network when accessing them for monitoring.

Consider **Claim 17,** and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for retrieving, from the first memory, at least one of a community name and a password for accessing the device using SNMP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use of SNMP along with passwords for monitoring devices in the network.

Consider **Claim 18**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for retrieving, from the first memory, an IP address of the device (Ramberg et al, [0046]). It clearly shows that the devices in the network have an IP address.

Consider **Claim 19**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the second memory comprises a vector of parameter name and parameter value paris for each of the plurality of communication protocols (Ramberg et al, [0055], [0056]). The SNMP subagents in Ramberg et al's invention uses routines as vectors, as they can used with other programs (Ramberg et al, [0055]). The routines are stored separately as files, and are pointed to when being used (Ramberg et al, [0055]).

Consider **Claim 20**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for storing step comprises: means for storing the

information for accessing the device in a device software object associated with the device (Ramberg et al, [0040], [0044]-[0045]). It clearly shows that device data is captured from the device and stored in a database.

Consider **Claim 21**, and as applied to claim 20 above, Ramberg et al clearly discloses wherein the device software object is stored in a random-access memory unit of a monitoring computer (Ramberg et al, [0051]). It clearly shows that during monitoring the application software is incorporating the use of system memory. The remote HTML browser which is the remote monitoring console runs on a computer, UNIX workstation, host computer etc. These systems have random-access memory unit to function properly (Ramberg et al, [0051]).

Consider **Claim 22**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: accessing the first memory using virtual functions associated with an abstract software class (Ramberg et al [0040]-[0041], [0047]). Ramberg et al clearly shows that the platform devices can be managed by the use of Dynamic User Inteface, as it uses XML. And the XML provides a data standard to encode the content, semantics, and schemata for communication. The Java system management can also be used (which contains classes) for communication with SNMP agents [0049].

Consider **Claim 23,** and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for accessing step comprises: means for transmitting to the device, information stored in the second memory necessary to access the device using the selected communication protocol (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows on the usage of memory on the system(s) when monitoring functionality is carried out when accessing the device(s) via SNMP.

Consider **Claim 24**, and as applied to claim 23 above, Ramberg et al clearly discloses wherein the means for accessing step comprises: means for receiving, by the device, the transmitted information; and means for processing, by the device, the received information (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows that during monitoring, both the system monitor and the monitored devices transmit information to each other and vice-versa.

Consider **Claim 25**, Ramberg et al clearly discloses a system of storing information configured to be used for a plurality of communication protocols to access a monitored device among distinct devices communicatively coupled to a network (Ramberg et al, [0024]), comprising: instructions of retrieving, from a first memory, information for accessing the device using at least one communication protocol supported by the device (Ramberg et al, [0038]) (It clearly shows that the management information base contains the information about the sets of objects, and providees information about each object – including its structure and relationship with other objects);

instructions of storing, in a second memory, the information for accessing the device retrieved from the first memory (Ramberg et al, Page 1, [0038]-[0039]) (There is also a MIB on the device, which tells SNMP ages information about the devices);

instructions for selecting a communication protocol among the plurality of communication protocols (Ramberg et al, Page 1, [0024], [0099]); and means for accessing the device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory (Ramberg et al, [0038]-[0039]). It clearly shows on how monitoring systems employ plurality of communication protocols to be used to monitor devices in the network. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 26**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: instructions for accessing a memory external to a monitoring computer to obtain the information for accessing the device (Ramberg et al, [0025], [0038], [0039]). It clearly shows on the use of remote computing system to monitor devices in the network. The management information base is also tied with the applications, which monitors the devices on the network via SNMP (Ramberg et al, [0039]).

Consider **Claim 27**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for selecting step comprises: means for selecting a communication protocol among SNMP, HTTP, and FTP (Ramberg et al, [0024], [0099]). It clearly shows that few of the protocols, which can be used for monitoring devices, comprises of the protocols SNMP, HTTP and FTP. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 28**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for retrieving step comprises: instructions for retrieving, from the first memory, at least one of a username and a password for accessing the device using FTP (Ramberg et al, [0078], [0094], [0099]). It clearly

shows on the use passwords on the devices in the network when accessing them for monitoring.

Consider **Claim 29,** and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for retrieving step comprises: means for retrieving, from the first memory, at least one of a community name and a password for accessing the device using SNMP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use of SNMP along with passwords for monitoring devices in the network.

Consider **Claim 30**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for retrieving step comprises: means for retrieving, from the first memory, an IP address of the device (Ramberg et al, [0046]). It clearly shows that the devices in the network have an IP address.

Consider **Claim 31**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the second memory comprises a vector of parameter name and parameter value paris for each of the plurality of communication protocols (Ramberg et al, [0055], [0056]). The SNMP subagents in Ramberg et al's invention uses routines as vectors, as they can used with other programs (Ramberg et al, [0055]). The routines are stored separately as files, and are pointed to when being used (Ramberg et al, [0055]).

Consider **Claim 32**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for storing step comprises: means for storing the information for accessing the device in a device software object associated with the device (Ramberg et al, [0040], [0044]-[0045]). It clearly shows that device data is captured from the device and stored in a database.

Consider **Claim 33**, and as applied to claim 32 above, Ramberg et al clearly discloses wherein the device software object is stored in a random-access memory unit of a monitoring computer (Ramberg et al, [0051]). It clearly shows that during monitoring the application software is incorporating the use of system memory. The remote HTML browser which is the remote monitoring console runs on a computer, UNIX workstation, host computer etc. These systems have random-access memory unit to function properly (Ramberg et al, [0051]).

Consider **Claim 34**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for retrieving step comprises: accessing the first memory using virtual functions associated with an abstract software class (Ramberg et al [0040]-[0041], [0047]). Ramberg et al clearly shows that the platform devices can be managed by the use of Dynamic User Inteface, as it uses XML. And the XML provides a data standard to encode the content, semantics, and schemata for communication. The Java system management can also be used (which contains classes) for communication with SNMP agents [0049].

Consider **Claim 35,** and as applied to claim 25 above, Ramberg et al clearly discloses wherein the instructions for accessing step comprises: instructions for transmitting to the device, information stored in the second memory necessary to access the device using the selected communication protocol (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows on the usage of memory on the system(s) when monitoring functionality is carried out when accessing the device(s) via SNMP.

Consider **Claim 36**, and as applied to claim 35 above, Ramberg et al clearly discloses wherein the instructions for accessing step comprises: means for receiving, by the device, the transmitted information; and means for processing, by the device, the received information (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows that during monitoring, both the system monitor and the monitored devices transmit information to each other and vice-versa.

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to:**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Anish Sikri whose telephone number is (571) 270-1783. The Examiner can normally be reached on Monday-Thursday from 6:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Rafael Pérez-Gutiérrez can be reached on (571) 272-7915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Anish Sikri
A.S./as

May 22, 2007